Vol.2009-IOT-6 No.7
2009/6/27

ISMS 文書の低コストかつ高効率な管理運用手法

長谷川　孝博[†1]　井上春樹[†1]　八巻直一[†1]

本論文では，国際規格 ISO/IEC27001 に基づく情報セキュリティマネジメントシステム (ISMS) で求められる文書管理術について，これを簡便かつ安価に実装する手法について提案する．本法は，ワードプロセッサやマインドマップなどの安価な汎用ツールを用いて，管理文書の機密性，完全性，可用性を大きく向上させることができる．本法は、ISO/IEC9000(QMS), 14000(EMS), 20000(ITSMS) や Jabee などの他規格へも応用可能である．

Inexpensive and effective techniques for the management and utilization of ISMS documents

Takahiro Hasegawa,[†1] Haruki Inoue[†1]
and Naokazu Yamaki[†1]

he International Organization for Standardization (ISO) set ISO/IEC27001 as the information security management system (ISMS). The requirements for ISMS documents are rather complicated and difficult to satisfy. Here we propose the set of simple, inexpensive and effective techniques that can be used easily in the management and utilization of ISMS documents. With these techniques, we can largely improve the confidentiality, integrity and availability of the documents. These techniques can be also applied to other standards, such as EMS, QMS, ITSMS and Jabee.

1. はじめに

本論文では，ISMS[1),2)] の構築初期段階で最初に直面する ISMS 最上位文書（ISMS マニュアル）や手順書の文書化およびその管理手法について，本学情報基盤センターでのこれまでの取組みを紹介することを目的とする．

ISMS 認証制度が，国内で開始された 2002 年当初，その認証基準は英国規格 BS7799 -2[3)] に基づいて行われていた．その後，BS7799-2 は ISO/IEC 27001：2005（2005 年 10 月）として ISO 化され，これが JIS Q 27001（2006 年 5 月）[1)] として JIS 化された．静岡大学情報基盤センター（2009 年 4 月に前身の総合情報処理センターから情報基盤センターへ改組，以下「センター」という）では，2003 年 11 月に BS7799-2 の認証取得を行った．当時，ISMS 認証規格制度が開始されてわずか 1 年ほどの初期でもあり，大学の情報系センターとしては ISMS 認証取得した初の機関であった．その後，センターでは，BS 規格と ISO 規格の差分構築を完了し，2007 年 10 月に ISO/IEC27001（JIS Q 27001）への切替え審査を完了し，認証 (2009 年 5 月現在) を維持している．本論文では，簡単のため，ISO/IEC 27001 と JIS Q 27001 を規格 27001，また実践規範をまとめる ISO/IEC 27002，JIS Q 27002[4)] を規格 27002 と呼ぶことにする．

ISMS 認証取得事業所数は 2009 年 5 月時点で 3169 団体であるが，このうち大学等の学術機関の認証取得数はわずか 1 桁程度に留まっている．その他は企業による認証取得である．この極端な割合は企業と大学の存在比率を考えれば，ある程度は妥当と言えるかもしれないが，学術機関の情報インフラの多様性や規模を考えれば，ISMS 認証取得まで完了するか否かは別にしても，ISMS 規格への理解は，より多くの教育機関へも波及して良いものと考える．

2. ISMS 文書化要求と分類

2.1 一　　般

規格書「第 4.3.1 項一般」の各要求事項 a)〜i）の 9 項目には，ISMS の基本方針および目的，適用宣言書，リスクアセスメント手法などに関する文書化の要求事項が列挙されている．文書化の意味，程度，手段については同項の注記 1, 2, 3 が重要である．注記 1 では，”文書化した手順”の意味を「その手順を確立し，文書化し，実施し，かつ，維持していること」と定義している．注記 2 では，文書化の程度が ISMS の活動の規模や種類や複雑さに応じて変化すること．注記 3 では，文書・記録の様式および媒体の種類は，どのようなものでもよいと記されている．特に注記 3 は，補助的な用紙媒体への出力はあるにせよ，主たる ISMS 文書の全てを電子ファイルのみで管理してもよいものと解釈できる．当センターの文書管理は，この注記を根拠として ISMS 文書の主体を電子文書で統合し，用紙媒体への出

†1 静岡大学情報基盤センター
Center for Information Infrastructure, Shizuoka University

力した文書群は補助的な位置付けとして運用している．

2.2 文書管理

規格書「第 4.3.2 項 文書管理」の各要求事項 a)〜j) の 10 項目には，文書の保護と管理に関する要求事項が列挙されている．各項目を要約は，a) 文書の承認，b) 文書のレビュー，c) 版管理，d) 改版状況の特定，e) 読みやすさ，識別の容易さ，f) 可用性の確保，g) 外部作成文書の識別，h) 配布管理，i) 廃止文書の誤使用防止，j) 廃止文書の識別に関するものであり，これらのことを確実に行うことが要件とされる．全体的には，ISMS が提唱する情報の機密性 (C: Confidentiality)，完全性 (I: Integrity)，可用性 (A: Availability) の観点から文書管理におけるセキュリティを求めている．従って，これら情報の CIA を満足する文書管理手法であることは重要である．

2.3 規格文書構造と文書管理手法

規格 27001 で規定される ISMS は，PDCA サイクルからなるプロセスアプローチを採用している．PDCA サイクルは Plan (計画: 確立)，Do (実行: 導入・運用), Check (点検: 監視・レビュー)，Act (処置: 維持・改善) の 4 フェーズを繰り返しながら組織のシステムを改善しつつ維持向上させる考え方である．その重要性は，規格書の階層構造そのものが，P, D, C, A の各フェーズで実施すべき事項を「第 4 章 情報セキュリティマネジメントシステム」配下の第 4.2.1 項，第 4.2.2 項，第 4.2.3 項，第 4.2.4 項に，記述していることからも読み取れる．後続の第 5 章から第 8 章には，これらに関連するより詳細な事項が記述されているに過ぎない．各項目の配下には，さらに 1 階層ないし 2 階層の連番を用いて，要件が詳述されている．

ISMS 認証には，規格書の全ての要件を充足する必要があるため，内部監査や外部審査機関による文書チェックは，規格書項目との 1 対 1 の対応関係に基づいて行われる．そのため，規格書構造に合致した文書レベル管理は指示された項目へのアクセスを容易にして，審査の精度と効率の向上にも寄与できる．また階層構造を守ることで，冗長記述や矛盾記述を見つけやすくなるという効果も得られる．従って，これらの規格文書の階層構造を守り，規格対応関係を明確にできる文書管理手法であることは重要である．

3. 文書管理手法

3.1 経　　緯

静岡大学情報基盤センターで確立してきた ISMS 上位文書の管理手法（以下,「本法」という）について述べる．本法が確立する以前には，ひとつの文書タイトルというだけの理由で細切にされた複数の電子ファイルで ISMS 上位文書が構成されていた．さらに，変更管理の結果生じたバックアップファイルに溢れ，文書内容の修正に掛ける数倍の時間をその電子ファイルの検索と真正性の確認に費やしていた．また，監査や審査において，文書の欠点や不適合を指摘される度に，その修正作業に要する作業時間は増大する一方であった．このような状況では，より高度な文書管理システムでこれらのファイルをとりまとめても，ファイルが分散しているがために生じる作業効率の悪さを容易に払拭できず，最悪の場合，文書管理の煩雑さと不完全さから，組織の ISMS の運営士気を低下させる恐れもある．事実，この事態を当センターでは経験して来た．

以上のような状況を踏まえて，ISMS 文書管理手法の抜本的見直しを行うに際し，1) 文書情報の CIA が高度かつ容易に維持できること，を重要視した結果，本法はワードプロセッサの編集機能を駆使しながら，徹底的なファイルの集約を行うという最も単純な方法に行き着いた．それゆえに本法は，2) 導入が安価で，3) 適用範囲にある全人員が文書の編集や管理に参加できる解りやすい手法にも成り得た．ここに ISMS が提唱する情報の CIA を適正に維持するという方針が，安価で解りやすい情報の管理手段を導いたことは重要であると考える．表 1 に文書ファイル集約の優位性を情報の CIA の観点からまとめた．

3.2 ファイルの集約とワードプロセッサ技法

複数に分散していた ISMS 上位文書ファイルを 1 つの電子ファイルに集約するという作業によって，語彙の揺らぎ，冗長記述，矛盾記述を排除して行くことが容易になる．その一

表 1 情報の CIA の観点で見た文書ファイル集約の優位性
Table 1 Advantages of Integrating documents on few files from th view of Information CIA.

観点	ファイル集約することの優位性
機密性 C	ファイル数が少なく，分散による漏洩を防止
	読込みと書き込みパスワードを区別して，編集権限を一括制御
完全性 I	ファイル数が少なく，表記の統一や真正性の確保が容易かつ正確
	表記の揺れを自動チェック，一括修正が容易かつ正確
	語彙の全置換機能による役職変更などが容易かつ正確
	目次生成が容易かつ正確
	変更管理や記録，差分出力が容易かつ正確
	用紙出力時の脱落頁がない
可用性 A	ファイル数が少なく，素早いアクセスが容易
	規格書の階層構造を文書レベルで再現，アクセスが容易
	目次や見出し機能により目的の文書へのアクセスが容易
	広範囲のキーワード検索が容易
	用紙出力が容易

方で，1 つのファイルの中に含まれる文書情報量（簡単に言えばページ数）は増えるため，これを効率よく管理する手段が必要となってくる．また，補助的とはいえ，監査や審査時には用紙出力が必要となるので，印刷時の見栄えも良いに越したことはない．

これらの要件を満たすため，本法では次のワープロ技法を主に活用した．

(1) 文書レベル機能

通常，9 段階の文書レベルに本文レベルを加えた 10 段階の文書階層をレベル分けすることができる．この機能を用いて，規格書と同じ階層構造を ISMS 上位文書に再現した．

(2) 見出し機能

文書レベルを設定することは，文書の目次生成を行うことと同等であり，これらは見出し機能によって別窓に伸展するツリー構造で表示することができる．文書全体を鳥瞰しながら，目的の文書に素早くアクセスできる．

(3) スタイルセット機能

スタイルセット機能は，文書レベルと文書スタイルを 1 対 1 に対応させることができる．1 つの ISMS 文書に適切なスタイルセットを作成することは手間を要する作業であったが，一度，このスタイルセットが完成すれば，文書修飾の作業から開放され，内容の編集に専念することができる．

(4) 段落番号リスト

文書階層に応じて，章・節・項，さらにその配下の段落番号まで自動管理できる連番機能を細部まで調整した．この段落番号リストも，スタイルセット同様，初回の調整には手間を要するが，一度作成してしまえば面倒な連番管理から開放される．

(5) アウトライン機能

文書レベルと密接に関連する機能であり，本来は，文書をアウトラインから記述して行くための機能であるが，数ページに跨る文書ブロックの単位で，まとめて文書位置を移動させる際に便利である．同じ書式で手順書を繰り返す規格 27002 の文書を作成，編集する際には特に有用であった．

3.3 ISMS 上位文書

当センターの ISMS 上位文書[⋆1]は，最終的に規格 27001 と 27002 の内容に沿って ISMS 上位文書を 2 つの電子ファイルに集約した．簡単のため，それぞれを文書 X，文書 Y と称することにする．文書 X，Y ともに規格書と同じ文書階層に自動連番を付して完全対応させた．

文書 X には，規格 27001 の 0〜8 章だけでなく，その中で文書化の要求が明記されている必須文書の他に，適用宣言書の表，リスク対応計画書，セキュリティ年間計画，さらには，1 枚から数枚で構成される各種様式を全て集約した．その結果，種々の様式や図表を包含する文書 X では，文書レベルに 1 対 1 の書式を完全適用することまでは困難となり，ある程度柔軟性を持たせて文書構造を管理した．また文書 X には，適用範囲のネットワーク図や建屋図などの CAD 系，Drow 系ソフトウェア作成した描画ファイルが含まれたが，これらもできるかぎりファイル数を集約した上で，最終的には文書 X の適切な位置にファイルオブジェクトとして埋め込み，見かけ上，文書 X のみの 1 つのファイルにまとめて管理した．図 1 に，文書 X の全体イメージと見出し機能による文書の階層構造を示す．

文書 Y には，規格 27002 に詳述される 133 の管理策の手順書，独自管理策の手順書を中心に 150 以上の手順書をまとめた．また，BS 規格と ISO 規格の差分項目として重点が置かれた管理策の有効性測定の評価も，情報の分散を防ぐ目的から 133 の管理策の配下に表形式で記述した．文書 Y では，文書全体に渡りほぼ例外なく文書レベルと書式の対応付けを行い，定型化をより明確にした．規格 27001 で指定される必須文書でも，文書 Y の強い定型に収まるものは，これらの文書グループにまとめて列挙した．強い定型を大量の文書に課すことは，すなわち，文書化の深さ，粒度や詳細さを揃えていくことに等しいので，文書全体の方針，ひいては ISMS の方針をより鮮明にできた．図 2 に，文書 Y の文書例と階層構造を示す．

3.4 変更管理

規格 27001 の第 4.3.2 項 文書管理の c) では，文書の改変を特定すること，および文書の改版状況の特定を確実にすることが求められている．監査や審査において，サンプリングチェックされる頻度の高い要件のひとつである．この要件は，ワープロの文書比較機能（差分解析）が極めて有効に活用できている．文書 X，文書 Y については，組織の ISMS が大きく変化しない限りにおいて，年 1 回の定期レビューを行っているが，通常の編集作業を文書全体に対して行い，複写しておいた 1 世代前の文書 X，文書 Y との差分解析を実施するだけで，要件に十分耐え得る変更出力が得られる．文書レベルの管理が厳密に実施されていることも解析精度が高くなる理由と思われる．また，この比較は，世代の異なる任意のファイルに対して動的に実施できるため，差分ファイルそのものを常時管理しておく必要はない．2009 年 4 月に当センターでは改組が実施され，ISMS 文書の大幅な改変が必要となったが，上位文書の主要な変更管理は，これを混乱なく円滑に完了することができた．

⋆1 一般には「ISMS マニュアル」と称する

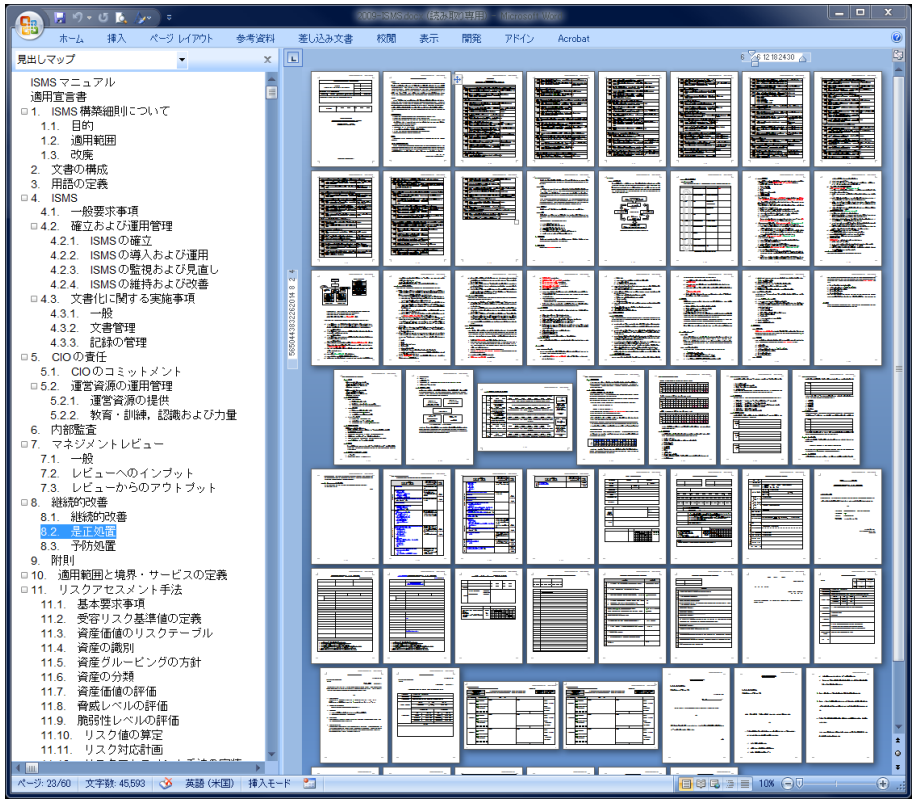

図 1 規格書の階層構造を文書レベルで再現した ISMS 上位文書 (文書 X)

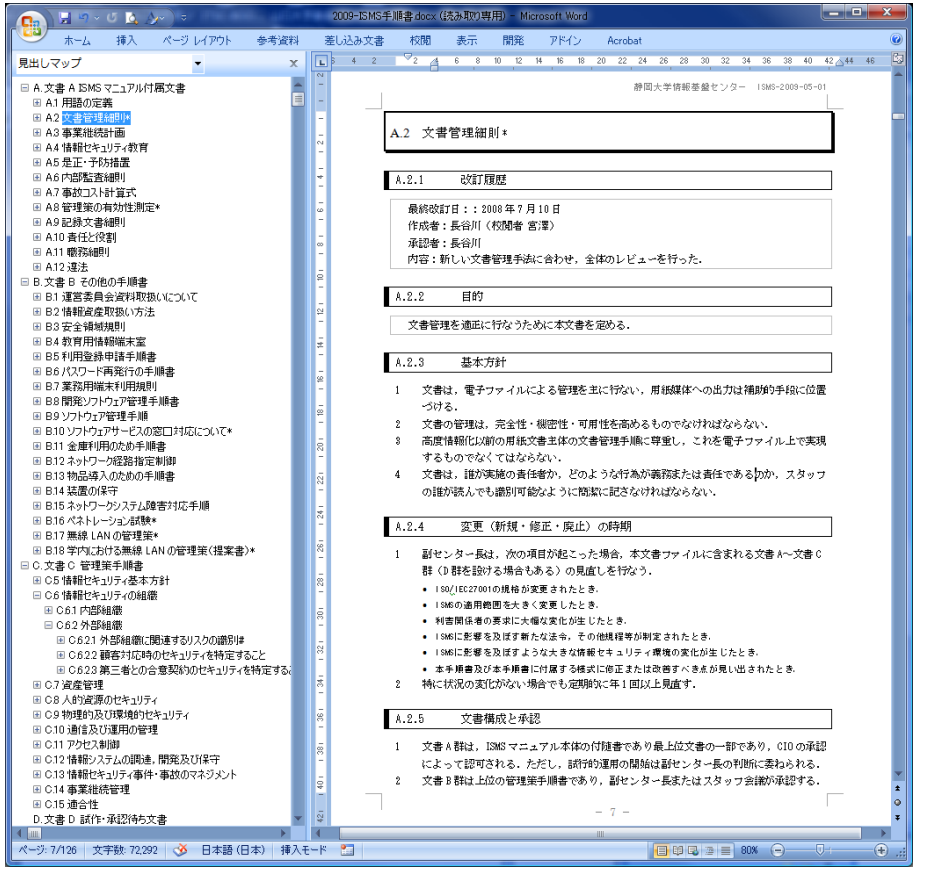

図 2 規格書の階層構造を文書レベルで再現した ISMS 上位文書 (文書 Y)：規格 27001 で必須となる上位文書 (A 群)，独自管理策の手順書 (B 群)，適用宣言した詳細管理策 (規格 27002) の手順書 (C 群)，未承認前文書 (D 群) で構成している．

4. マインドマップによるリスクアセスメント表記法

4.1 リスクアセスメント

ISMS 上位文書には，規格 27001 の第 4.2.1 項に詳述されるリスクアセスメント[5),6)] の結果も含まれる．ISMS では，特定した事業上の情報セキュリティや法令および規制の要求事項に適したリスクアセスメントを特定し，文書化し，これを実装しなければならない．リスクアセスメントの方法例については TR X 0036-3[7)] や ISMS ユーザーズガイド[8)] に示される．たとえば，ISMS ユーザーズガイドでは，ベースラインアプローチ (Baseline Approach)，非線形的アプローチ (Informal Approach)，詳細リスク分析 (Detail Risk Anaylsis)，組合せアプローチ（Combined Approach) が紹介されている．当センターでは，詳細リスク分析を主とするが，これだけでは作業量的に補いきれない部分にベースラインアプローチと非線形的アプローチを充てる組み合わせアプローチによるリスクアセスメントを実施している．

4.2 詳細リスク分析

詳細リスク分析では，まず，1 つの情報資産またはグループ化された 1 つの情報資産群に対して，機密性，完全性，可用性の観点からその資産価値を数量化する．次に，その資産の価値を損失するかもしれない脅威を全て特定し，その脅威がつけ込むかもしれない脆弱[⋆1]も全て洗い出し，おのおの程度を数量化する．これらの 3 つの数値の積，すなわち (資産価値)×(脅威レベル)×(脆弱レベル) からその資産が持つリスクの 1 つを算定する．1 つの情報資産には CIA の観点から 3 つの資産価値が評価され，おのおのに，複数の脅威が取り巻き，さらに 1 つの脅威がつけ込むかもしれない脆弱も複数存在する場合もある．そのため，詳細リスク分析では，1 つの情報資産が複数の独立したリスク値を有しており，この結果を柔軟に記述するための文書化の工夫が必要である．また，正確さや解り易さの他に，継続的なレビューや作業分担の容易さなども考慮されるべきである．

4.3 マインドマップ

詳細リスク分析によるリスクアセスメントの結果のデータ構造の特殊性に鑑み，これを文書 X と文書 Y とは全く異なる方法で記述することを考えた．マインドマップ[9)] は，放射状のチャートに自由なアイデアを展開しながら，思考を整理していく画期的なツールとして近年脚光を浴びてきた．著者らは，ソフトウェア化されたマインドマップの伸縮するツリー構造が，詳細リスク分析の結果が持つ複雑なツリー構造を柔軟かつ多彩に表記できることに着目し，その表記法を ISMS 運用の中で確立して来た．また，マインドマップは，安価 (ビュアは無料) であり，操作の解り易さもワープロと同程度に備えている．リスクアセスメント結果のマインドマップによる表記例については文献[5)] がある．図 3 には，リスクアセスメントにおいて必須となる脅威とそれにつけ込むかもしれない脆弱のマップを示す．また，マインドマップは汎用ツールであるため，その表記の柔軟性に着目すれば，ISMS においても様々な活用が期待できる．当センターでは，脅威と脆弱の関係図，規格書 27001，規格書 27002，スタッフの構成図などもマインドマップで描いている．これらは，ISMS の規格構造や規模を視覚に訴える説明ができるため，スタッフ教育でも有効に活用している．マインドマップの欠点として，汎用ツールが故に，大規模な ISMS の資産管理やリスクアセスメント管理には有用と思われるデータベース機能やリスクの演算機能を備えていないことが挙げられる．適切なグルーピングを行った資産数 300 程度が，導入効果を期待できる管理規模の上限と考えている．

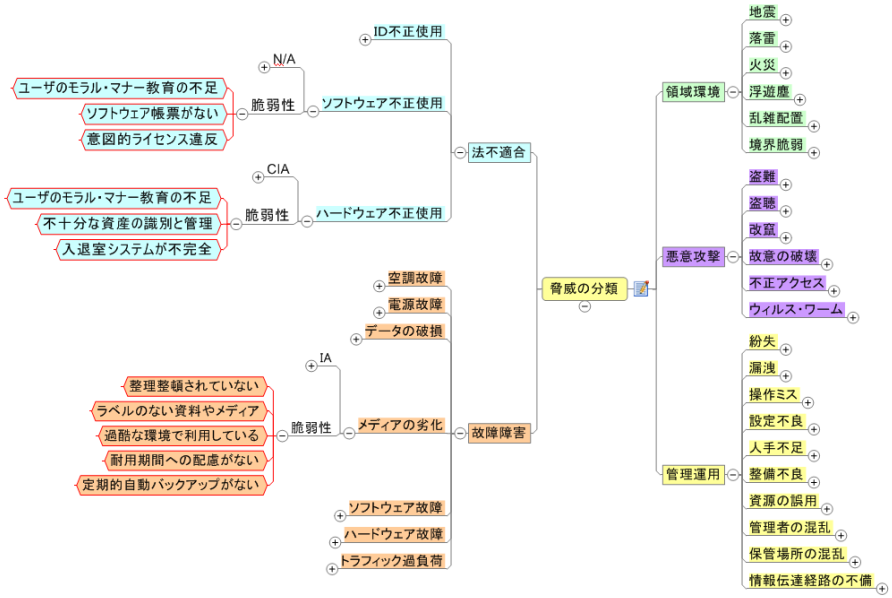

図 3 マインドマップによる脅威と脆弱の関係図

⋆1 「それ (脅威) につけ込むかもしれない脆弱」とは規格で用いられている独特の表現である．

5. ま と め

静岡大学情報基盤センターにおける ISO/IEC27001 の国際規格に基づく ISMS 上位文書の管理手法について述べてきた．当センターでは，ISMS 認証当初の煩雑であった ISMS 上位文書の分散ファイルによる管理を見直し，安価な汎用ツールとその機能を活用して徹底したファイル集約を行ってきた．その結果，ISMS 文書管理の CIA の向上を実現することができた．ISMS 上位文書は，現在のところ 2 つのワープロファイル（文書 X と文書 Y）と，1 つのマインドマップに集約されている．これらのファイル数には 3 年以上変化はなく，キャンパス間の共有ドライブの最上位に常に最新版を配置している．これにより上位の文書管理システムの必要性も感じることなく，また，監査や審査においても文書管理に関する高い評価を維持している．

本法は，高価な文書管理システム等の導入を行う前に，十分検討に値する安価な汎用手法である．スタッフの技能に依存することなく，全員参加型の文書構築と管理の効率化が期待できる．規格 27001 に限らず，ISO/IEC 9000(QMS), 14000(EMS), 20000(ITSMS), Jabee(日本技術者教育認定制度) などの認証取得や，身近なところでは社内文書管理でもよき指針を与えるものと期待している．

謝辞 本成果は静岡大学情報基盤センタースタッフの多大なる協力のもとに行われました．ここに記して謝意を表します．

参 考 文 献

1) JIS Q 27001: 2006 (ISO/IEC 27001:2005): 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム要求事項，日本規格協会 (2006).
2) 長谷川孝博，伊藤賢，井上春樹，八巻直一：実践 ISMS 講座，静岡学術出版 (2007).
3) BS 7799-2:2002: 情報セキュリティ管理システム仕様，日本規格協会 (2001).
4) JIS Q 27002: 2006 (ISO/IEC 27002:2006): 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステムの実践のための規範，日本規格協会 (2006).
5) 長谷川孝博，伊藤賢，市川哲彦，永井好和，三池秀敏，井上春樹，八巻直一：ISMS における詳細リスク分析の半自動化手法と WEB システムへの実装，リスク研究学会 第 21 回年次大会発表予稿集論文集， No.12, pp.177–182 (2008).
6) 市川哲彦，永井好和，長谷川孝博，伊藤賢，三池秀敏：情報セキュリティマネジメントシステム (ISMS) における効率的な詳細リスクアセスメント実施手法の提案と情報処理センターへの適用，学術情報処理研究， No.12, pp.52–58 (2008).
7) TR X 0036-3:2001: IT セキュリティマネジメントのガイドライン－第 3 部: IT セキュリティマネジメントのための手法，日本規格協会 (2001).
8) ISMS ユーザーズガイド，日本情報処理開発協会 (2006).
9) Buzan, T. and Buzan, B.: *The Mind Map Book*, BBC Active (2006).